UNIVERSITY OF DETROIT MERCY

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

NOTICE OF DATA BREACH

[redacted]

[redacted]

Dear [redacted]:

We are writing to let you know about a data security incident at Blackbaud, a third-party vendor. Blackbaud is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at non-profits and universities around the world, including University of Detroit Mercy ("Detroit Mercy").

Detroit Mercy takes the protection and proper use of your information very seriously. We are therefore contacting you out of an abundance of caution to explain the incident and timely provide you with the information that Blackbaud has provided its customers.

What Happened

On July 16, 2020, Blackbaud notified Detroit Mercy of a ransomware attack on their internal systems. Upon learning of the issue, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents.

Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud engaged forensic experts and law enforcement to assist in their internal investigation. The investigation concluded that the cybercriminal removed data from Blackbaud's systems intermittently between February 7, 2020 and May 20, 2020. A backup file containing certain information was removed by the cybercriminal. According to Blackbaud, they paid the cybercriminal to ensure that the backup file was permanently destroyed.

What Information Was Involved

On July 31, 2020, we determined that the information removed by the threat actor may have contained your full name and Social Security number. **The threat actor did not access your payment card information or bank account information because Detroit Mercy does not store this information in the Blackbaud database.**

What Blackbaud Is Doing

Blackbaud has stated that their teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They indicate they have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do

Again, according to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not impact your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices, and those of our third party services providers, to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

University of Detroit Mercy

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <[redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code**: <[redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted]

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.